WHAT IS CLAIMED:

1. An apparatus for detecting whether router status information sent from a first router is unreliable, comprising:

a memory for storing a router status database; and

a processor which (i) receives a first signal corresponding to a first router status message sent by the first router, the first router status message containing router status information indicative of the status of communication between the first router and a second router, (ii) compares the received first signal with a second signal stored in said router status database, the second signal corresponding to a second router status message sent by the second router, the second router status message sent by the second router, the second router status message containing router status information indicative of the status of communication between the second router in the first router, and (iii) issues an alarm signal if the signal comparison reveals that the first and second router status messages contain non-complementary router status information.

2. An apparatus according to Claim 1, wherein said apparatus is incorporated into the second router.

3. An apparatus according to Claim 1, wherein said processor waits a predetermined period of time after receiving the first signal before

performing the signal comparison.

4. An apparatus according to Claim 1, wherein the processor performs the signal comparison by determining if both the first and second signals indicate that the link between the first and second routers is operational.

5. An apparatus according to Claim 1, wherein said processor, after the signal comparison, (i) waits a predetermined period of time, (ii) receives renewed first and second signals, and (iii) reperforms the signal comparison on the basis of the renewed first and second signals.

6. An apparatus according to Claim 1, wherein the processor issues the alarm signal in a third router status message transmitted to at least the second router.

7. An apparatus for detecting false routing updates issued from a compromised router, comprising:

a memory which stores a router database that contains an entry corresponding to a router update received from another router and characterizing the link status between the another router and the compromised router; and

a processor which (i) receives a signal corresponding to a router update received from the compromised router and characterizing the link status between the compromised router and the another router, (ii) compares the received signal with the entry stored in the router database, and (iii) issues an alarm signal if the received signal and the database entry contain non-complementary link status information regarding the link between the compromised router and the another router.

8. An apparatus according to Claim 7, wherein said processor issues a router update if said processor determines that the received signal and the database entry contain complementary link status information regarding the link between the compromised router and the another router.

9. An apparatus according to Claim 7, further comprising a receiver for receiving the router update from the compromised router, and a transmitter for transmitting the alarm signal.

10. An apparatus according to Claim 7, wherein said apparatus comprises the another router.

11. A method for detecting whether router status information sent from a first router is unreliable, comprising the steps of:

storing a router status database;

receiving a first signal corresponding to a first router status message sent by the first router, the first router status message containing router status information indicative of the status of communication between the first router and a second router;

comparing the received first signal with a second signal stored in said router status database, the second signal corresponding to a second router status message sent by the second router, the second router status message containing router status information indicative of the status of communication between the second router in the first router; and

issuing an alarm signal if the signal comparison reveals that the first and second router status messages contain non-complementary router status information.

12. A method according to Claim 11, wherein said method is performed in the second router.

13. A method according to Claim 11, further comprising the step of waiting a predetermined period of time after receiving the first signal before performing the signal comparison.

14. A method according to Claim 11, wherein the signal comparison is performed by determining if both the first and second signals indicate that the link between the first and second routers is operational.

15. A method according to Claim 11, further comprising the steps of, after the signal comparison:

waiting a predetermined period of time;

receiving renewed first and second signals; and

reperforming the signal comparison on the basis of the renewed first and second signals.

16. A method according to Claim 11, wherein the step of issuing the alarm signal comprises the step of issuing the alarm signal in a third router status message transmitted to at least the second router.

17. A method for detecting false routing updates issued from a compromised router, comprising the steps of:

storing a router database that contains an entry corresponding to a router update received from another router and characterizing the link status between the another router and the compromised router;

receiving a signal corresponding to a router update received from the compromised router and characterizing the link status between the compromised router and the another router;

comparing the received signal with the entry stored in the router database; and

issuing an alarm signal if the received signal and the database entry contain non-complementary link status information regarding the link between the compromised router and the another router.

18. A method according to Claim 17, further comprising the step of issuing a router update if said processor determines that the received signal and the database entry contain non-complementary link status information regarding the link between the compromised router and the another router.

19. A method according to Claim 17, further comprising the step of broadcasting the alarm signal.

20. A method according to Claim 17, wherein said steps are performed in the another router.

21. A storage medium containing computer-readable code which causes one or more router processors to perform a method for detecting whether router status information sent from a first router is unreliable, the computer-readable code causing the one or more router processors to perform the functions of:

storing a router status database;

receiving a first signal corresponding to a first router status message sent by the first router, the first router status message containing

router status information indicative of the status of communication between the first router and a second router;

comparing the received first signal with a second signal stored in said router status database, the second signal corresponding to a second router status message sent by the second router, the second router status message containing router status information indicative of the status of communication between the second router in the first router; and

issuing an alarm signal if the signal comparison reveals that the first and second router status messages contain non-complementary router status information.

22. A storage medium containing computer-readable code which causes one or more router processors to perform a method detecting false routing updates issued from a compromised router, the computer-readable code causing the one or more router processors to perform the functions of:

storing a router database that contains an entry corresponding to a router update received from another router and characterizing the link status between the another router and the compromised router;

receiving a signal corresponding to a router update received from the compromised router and characterizing the link status between the compromised router and the another router;

comparing the received signal with the entry stored in the router database; and

issuing an alarm signal if the received signal and the database entry contain non-complementary link status information regarding the link between the compromised router and the another router.

23. An apparatus for detecting whether router status information sent from a first router is unreliable, comprising:

means for storing a router status database; and

means for (i) receiving a first signal corresponding to a first router status message sent by the first router, the first router status message containing router status information indicative of the status of communication between the first router and a second router, (ii) comparing the received first signal with a second signal stored in said router status database, the second signal corresponding to a second router status message sent by the second router, the second router status message containing router status information indicative of the status of communication between the second router in the first router, and (iii) issuing an alarm signal if the signal comparison reveals that the first and second router status messages contain non-complementary router status information.